软件安全需求获取方法的研究

金 英 刘 鑫 张 晶
(吉林大学计算机科学与技术学院 长春 130012)

摘 要 近年来,软件主动式防御思想在软件安全性保障中的地位越来越高,它是一种积极的保障软件安全性的思想,可有效地构建高可信性软件。安全需求的获取是软件安全性保障中最关键的部分,是主动式防御首要完成的任务并且也是最难完成的部分。针对典型的安全需求获取方法,从它们的研究途径、应用情况等方面进行比较和分析,总结并讨论了安全需求获取方法的状况及其未来的发展趋势。上述工作将对安全需求获取方法的研究和实践应用提供有益参考。

关键词 软件安全性,主动式防御,安全需求,威胁
中图法分类号 TP311 **文献标识码** A

Research on Eliciting Security Requirement Methods

JIN Ying LIU Xin ZHANG Jing
(College of Computer Science and Technology, Jilin University, Changchun 130012, China)

Abstract Recently more and more attention has been paid to use active defense in software security because it provides a positive way to guarantee software security and effectively construct high-confidential software. Security requirements were critical to software security assurance. Eliciting security requirements was one of major and difficult tasks during the security assurance. Some typical methods about eliciting security requirements were studied, compared and analyzed with respect to their research methods, application, etc. The current status of different approaches to security requirements elicitation were summarized, and future trends were explored in the end. The above work will provide a valuable reference for carrying out research and application in security requirement engineering.

Keywords Software security, Active defense, Security requirements, Threat

1 引言

软件安全性早在20世纪90年代就被计算机科学家们公认为是21世纪软件研究和发展的重要战略方向之一[1]。软件安全性可简单概括为:软件在任何情形下都不能使其控制的系统对人们的生命、财产及其所处的自然环境造成危害[1]。

软件安全性是一个系统问题。软件在其应用系统中一方面协调系统的各个部分有效地工作,另一方面又可能使系统进入危险状态。以放射性治疗系统的软件为例,其存在的错误已致使多国的癌症病人遭受过量辐射而死亡[1]。

软件安全性是软件开发中所面临的难题。先进的软件构建技术(COBRA技术、NETWARE技术等)一方面能满足软件商业化的利益要求,灵活地扩展软件的服务功能;另一方面又给软件造成了安全漏洞,尤其是分布式软件构建技术。

目前用以保障软件的安全性的解决方案共有两种模式:主动式防御和被动式防御。被动式防御的主要思想是在软件开发后期弥补软件所需的安全性功能,通过第三方获取安全支持或者添加安全功能模块。这种解决方案主要存在以下两个缺点:

1)第三方的安全支持很少是为软件量身定制的,如杀毒软件。因此它只能解决一般性的安全问题,不能较好地解决具体软件的安全性问题。

2)安全功能模块的添加不仅需要对软件进行修改和重构,耗费大量的人力、时间和成本,而且这个过程中还可能产生新的安全问题。

主动式防御思想是从系统自身出发,在软件开发的需求阶段就捕获系统的安全需求,将安全需求作为一项安全契约用以指导软件开发后期的设计、实现和测试,使得软件开发的各个周期都有安全性保障。主动式防御避免了被动式防御存在的缺点,能够有效地开发高安全性、高可信性的软件产品。

安全需求的获取任务是软件主动式防御的基础和关键,它作为一项契约将直接影响软件后续阶段的安全性保障,是保障软件安全性的决定因素。然而,安全需求的获取是最难完成的部分,其主要困难有:

到稿日期:2010-04-17 返修日期:2010-07-19 本文受国家"863"高技术研究发展计划专题课题(2007AA01Z123),国家自然科学基金青年基金(60603031),吉林大学科学前沿与交叉学科创新项目(200903193)资助。

金 英(1971—),女,教授,CCF会员,主要研究方向为需求工程、软件形式化技术、移动代码安全等;刘 鑫(1985—),男,硕士生,主要研究方向为安全需求工程等;张 晶(1975—),女,讲师,主要研究方向为需求工程、程序分析技术、软件形式化方法等,E-mail:zhangjing99@jlu.edu.cn(通讯作者)。

(1)软件安全问题的产生难以预料；

(2)应用领域安全问题的多样性；

(3)客户安全需求的模糊描述和多变性。

本文主要阐述了软件安全需求获取的主要思想，选取当前典型安全需求获取方法和技术，从它们的研究途径、适用范围、应用情况等方面进行比较和分析，总结并给出了今后的发展趋势。本文第2节全面阐述安全需求的含义、获取过程、所需支持和技术；第3节阐述安全需求获取的基本途径，对选取的典型方法进行分类和分析比较；第4节讨论现有方法中存在的问题以及安全需求获取的发展趋势；最后做全文总结。

2 安全需求

2.1 安全需求的含义

在明确安全需求含义之前，先介绍几个相关的概念。

1)资产[2]：系统所包含的资源和信息。

2)威胁[2]：对资产造成危害的潜在行为。

3)安全目标[2]：应对威胁的意图说明，可以满足系统的安全需要。

4)安全漏洞[2]：系统的弱点或缺陷，被攻击者利用而违背资产的安全目标。

5)安全需求[3]：对功能性需求的约束，消除资产存在的安全漏洞。

概念5)具有的含义：安全需求是指系统应该“做什么”来满足安全目标，消除软件系统的安全漏洞。安全需求的语义描述中应避免“如何去做”的出现。

威胁是安全需求获取的关键，通过分析认为共有两个来源可导致威胁发生，一是软件开发人员在设计与实现过程中出现的纰漏和错误，另一个是系统开发人员对软件面临的安全问题考虑得不够完整、不够充分。前者产生的威胁是软件开发过程中人力所不能避免的；后者是软件系统产生安全问题的主要根源，获取软件的安全需求正是为了消除这一根源。针对来源二进一步分析，它可引发两种情形的威胁：

1)软件正常使用者引起的安全问题，比如合法用户的疏忽操作导致的信息泄露；

2)恶意地攻击软件系统，比如病毒攻击、木马攻击。

获取安全需求的目的就是要避免这两种威胁的发生。目前安全需求的获取方法主要是针对情形2)展开研究，这也是本文的工作方向。

2.2 获取过程

对典型的安全需求获取方法进行了总结，安全需求获取过程如图1所示。

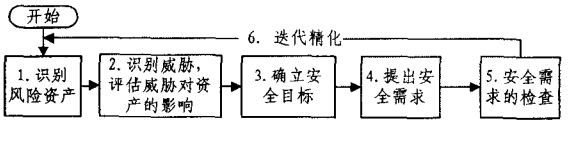

图1 安全需求获取过程图

本文虽从不同角度介绍了安全需求获取方法，但这些方法的框架都包含这6个步骤。其中迭代精化步骤是该过程的核心，越精化的安全需求越有利于说明系统实际存在的安全问题。

2.3 所需支持和研究内容

在安全需求获取过程中，需要3个方面的支持，即安全知识背景、技术手段、获取工具。安全知识背景是安全需求获取的基础，一个具有安全知识背景的团队能够更好地沟通协作，有利于软件安全性保障的实践。技术手段是获取安全需求的关键，好的技术能够便于人们发现系统面临的威胁并提取安全需求。获取工具是安全需求获取过程的必要支持，可视化、文档化、自动化或者半自动化分析工具有利于分析人员快速、高效地获取安全需求。这3方面支持缺一不可，它们是获取安全需求的支撑框架。

安全需求获取方法主要从3个方面进行研究，获取技术的研究、组织描述方法的研究和验证技术的研究。

(1)获取技术主要包含威胁获取技术和安全需求提取技术的研究。目前，获取技术的研究主要基于两种思想，思想1：研究出一套威胁分析策略和安全需求提取手段，用于指导安全分析人员获取安全需求，安全分析人员依据自身的经验确定软件系统的安全威胁和安全需求。思想2：基于安全知识复用的思想，通过对软件所遭受的安全威胁及其安全需求解决方案进行建模，将建立的模型作为复用的知识资源，其他软件开发团队可复用它们来获取安全威胁和安全需求，这种思想较少依赖安全分析人员确定安全威胁和安全需求。

(2)组织描述技术主要是关于威胁和安全需求的组织和描述技术。安全威胁的良好组织和描述将有利于软件开发相关者们更好地理解系统面临的安全问题，能够有力地说明安全需求制定的动因，安全威胁的组织描述目前有采用攻击树、面向方面的组织形式等。安全需求的良好组织和描述将有利于开发人员实施系统安全方面的设计，目前主要有用例、问题框架等安全需求组织描述技术。

(3)验证技术主要是检验安全需求之间的冲突、安全需求与系统功能需求之间的冲突等，验证安全需求是否满足用户方的期望，证实安全需求是完备的、有效的。安全需求的验证技术可以采用模型检查器、模型解释器(图表、符号执行)、快速原型生成器等需求验证技术。

3 安全需求分析的基本途径

3.1 基本研究途径

安全需求获取方法目前主要从两个基本途径展开研究：一是在已有的需求分析方法上研究如何获取安全需求，弥补原有需求分析方法在获取安全需求方面的不足。二是抛开已有的需求分析方法，针对软件安全这一特殊需求，研究特定的安全需求获取方法。目前采用第一种途径的研究工作较多，第二种途径的研究工作较少。

3.2 典型方法分类

本文考察了如下安全需求获取方法，并对这些方法按照研究途径和获取安全需求的思想进行分类，如表1所列。

表1 典型安全需求分析方法分类

途径1：已有需求获取方法上的扩展	途径2：特定的方法
1.(用例)Misuse case[4,5]，Abuse case[6]	6. CLASP[13]
2.(问题框架)Abuse frame[7,8]	7. CC[14,15](复用的思想)
3.(面向目标)Anti-models[9]	
4.(面向主体和意图)Security I * /Tropos[10]	
5.(面向方面)crosscutting threaten[3,11,12]	

途径1中将一些方法按照其扩展依据进行归类，比如Misuse case，Abuse use case这两个方法都是基于用例需求分析方法提出的安全需求获取方法。表中方法7是基于安全知

识复用的思想研究得到的，其余的方法都是基于获取思想 1 研究得到的。

3.3 典型方法介绍及评价

对所选取的方法先进行必要的介绍，然后从方法的可用性、适用性、安全需求获取的有效性和完整性、安全需求的描述形式、安全需求的被复用情况等方面进行分析和比较。

1)可用性：方法使用的难易程度。

2)适用性：方法适用的上下文环境。

3)有效性：所获取的安全需求是否有效。

4)完整性：所获取的安全需求是否完整。

5)描述形式：采用的描述形式，比如自然语言、形式化、半形式化等。

6)复用情况：方法的执行结果中是否有可复用的资源作为领域内的安全知识。

3.3.1 滥用用例

传统的用例分析方法主要用于分析获取软件系统的功能性需求，它不能够用于捕获软件系统的安全需求。滥用用例方法的提出弥补了这一缺点，其主要思想是：从恶意攻击者的角度考虑系统面临的威胁，分析系统存在的安全漏洞，建立威胁用例，针对威胁用例建立安全需求用例。滥用用例的典型性方法有 Misuse case，Abuse case。

Misuse case 主要从功能性用例的文本描述中分析可能存在的安全漏洞并识别出对应的威胁，建立威胁用例，针对威胁用例建立安全需求用例。Sindre 和 Opdahl 等人给出了威胁用例的组织形式和内容[4]；Firesmith 等人对一些典型的安全问题给出了安全需求用例的组织形式和内容[16]。在 Misuse case 方法中，还定义了新的关系：threatens 用来表示威胁用例能够对功能性用例造成威胁；detects 用来表示用例对威胁的监测；prevents 关系用来表示安全需求用例可以阻止威胁用例被实施；mitigates 关系用来表示安全需求用例可以缓解威胁用例所产生的危害效果。目前 Misuse case 方法已有工具支持。

Abuse case 方法主要用于捕获攻击者与系统之间的交互所产生的威胁。该方法重视对攻击者的描述，主要对攻击者的企图、攻击能力进行评估。为了识别安全隐患，方法从系统的全局出发，对系统的各个部分进行考察，寻找安全漏洞并建立漏洞攻击树[6]。Abuse case 方法针对识别出的威胁，单独建立威胁用例，与 misuse case 方法不同的是：建立好的威胁用例并不与功能性用例产生交互，威胁用例仅说明系统面临的安全威胁。威胁用例的描述形式既可以采用已有的用例模板，也可采用漏洞攻击树。该方法采用 UML 用例建模工具作为支撑工具。

以上所介绍的两个方法都有相应的支持工具，因此它们的可用性较好。它们比较适用于对已有的用例需求文本进行分析，以获取安全需求。这两个方法虽然给出了威胁分析方法，但威胁用例和安全需求用例的确定需要依靠经验丰富的安全分析人员。威胁用例的建立到安全需求用例的建立是一个因果过程，这使软件系统的相关利益者可以很好地理解系统所面临的安全问题。威胁用例和安全需求用例可作为领域内的复用资源，作为安全知识，可被其他软件开发者所使用。

3.3.2 滥用问题框架

滥用问题框架方法(abuse frame)是对问题框架方法的扩展，从攻击者的角度考虑系统面临的安全问题。方法中定义了“攻击者领域”，用来表示攻击者；定义了“受害领域”表示系统遭受威胁的资产；引入了“反需求”概念，“反需求”表示攻击者对系统的需求，这样的需求违背了系统正常、合法的需求。该方法与问题框架法的本质区别是：它先获取反需求，然后再制定相应的安全需求；而问题框架方法在分析安全需求时与分析系统的其他需求一样，直接进行问题领域和机器领域的现象分析，然后得到需求，因此问题框架分析方法较少能获取“反需求”。

滥用框架的威胁获取主要从两个方面入手：

1)问题领域内的现象。由于现象描述缺乏安全性约束，使得安全漏洞可能显式或隐式地存在于现象中。

2)领域之间的现象交互过程。其存在的安全隐患经常是外部攻击的切入点。

Abuse frame 方法中引入 abuse frame 描述反需求，如图 2 所示。

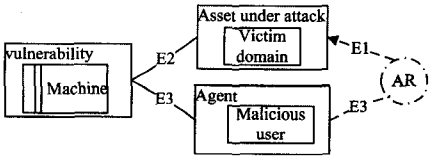

图 2 abuse frame 威胁描述图

图 2 中 AR 表示“反需求”，Victim Domain 表示“受害领域”，Malicious user 表示“攻击者领域”，Machine 表示“机器领域”。现象 E1 表示 AR 在 Victim Domain 产生的安全威胁现象；E2 表示机器领域与 Victim Domain 之间的共享现象，机器领域通过 E2 对 Victim Domain 进行操作，来完成软件系统的功能。实线形状的 E3 表示恶意攻击者对机器领域产生的攻击现象；虚线形状的 E3 表示 AR 到“攻击者领域”的需求引用，它和 AR 一起描述了“攻击者领域”对机器领域的攻击效果。

针对 AR，滥用框架方法用 problem frame 描述安全需求，如图 3 所示。

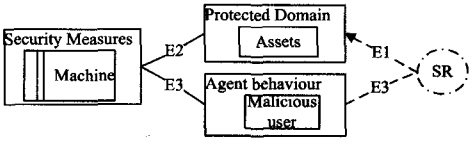

图 3 安全需求描述图

图 3 中 SR 表示安全需求，E1 表示在攻击情形下受保护领域所期望的现象。E2，E3 的含义与图 2 一致。

滥用问题框架法可采用已有的问题框架方法支持工具分析和获取安全需求。该方法是一种面向问题域的分析方法，适合针对问题领域进行分析，获取安全需求。方法虽然提供了威胁分析途径，但还需要有经验的安全人员从现象的描述中确定威胁，他们的经验和能力决定了安全需求的有效性和完整性。Abuse frame 图和安全需求描述图能够体现系统面临的安全问题。Abuse frame 中各个领域的现象描述以及领域之间的现象描述可作为安全知识帮助同领域内的其他软件系统确定安全威胁，而 problem frame 中安全需求的描述也可作为复用资源来帮助制定同领域的软件系统的安全需求。

3.3.3 反模型

反模型(Anti-models)方法是针对面向目标的需求分析

方法不能捕获由恶意的攻击行为所产生的障碍目标的缺点而给出的恶意障碍目标获取方法和消解恶意障碍目标的方法。该方法是 Axel 等人提出的，他们引入了反目标的概念，用反目标(anti-goals)代表具有恶意性质的障碍目标；他们还对传统的 KAOS 框架进行了扩展，引入了认知时序逻辑结构和模式，以支持反目标的形式化分析和推理。

反模型方法获取安全需求的主要过程如下：

1)从系统中找出一些安全关键性的对象并为它们定义安全关注点。用扩展的 KAOS 语言形式化描述这些安全关注点，对形式化的安全关注点进行语义取反，得到初始的反目标。

2)分析初始的反目标，识别出具有反目标意图的攻击者。

3)进一步分析攻击者的动机，尽量获取攻击者的真实动机，得到更多的反目标。

4)精化步骤 3)所得到的反目标，直到反目标可被攻击者直接实施或者可具体化为软件的防御漏洞。该步骤可采用目标回归法、模式精化法对反目标进行精化。

5)根据反目标，建立攻击者与软件系统之间的“反模型”。

6)消解反目标，主要采用反目标弱化、反目标消除等手段，这些手段可作为安全目标。

从上述过程中可以看出，反目标的形式精化过程需要数学推理能力较强的人来实施，从而保证反目标获取结果的正确性、有效性和完整性。因此该方法适合安全经验丰富、对面向目标的需求获取方法较熟悉的开发团队来使用。该方法主要有两个缺点，一是反目标形式化的描述可读性较差；二是需求的变化将导致之前获取的反目标可能变得完全无效，反目标推理过程需要重新开始，这使反目标不容易被复用，安全目标也不容易复用。

3.3.4 安全的 I*/Tropos

传统的面向主体与意图需求分析方法几乎很少涉及安全需求的捕获，而主体建模活动中往往存在安全隐患。目前主要的面向主体和意图的方法是基于 I* 建模框架的 Tropos 方法，基于主体和意图获取安全需求的方法主要是在 I* 和 Tropos 方法中引入安全约束机制，用来保护模型中可能遭受安全威胁的任务、目标、资源、软目标和依赖关系。典型性方法是刘璘等人提出的基于社会背景的安全与隐私的需求分析方法。

刘璘等人提出的方法以 I* 建模活动为基础，考察正常的 I* 建模活动的每一步骤，从攻击者的角度考虑步骤中存在的安全隐患，并为安全隐患制定消除机制，提出安全需求。该方法获取安全需求的主要过程如图 4 所示。

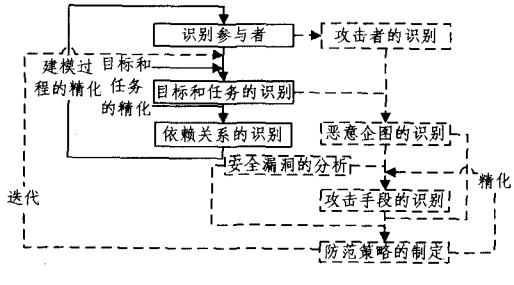

图 4 基于 I* 框架的安全与隐私需求的获取过程图

图 4 中左边实体部分为 I* 正常建模需求的过程，右边的虚线部分为方法获取安全需求的过程。

刘璘等人的方法利用主体建模活动中的策略推理模型和策略依赖模型，将威胁的分析通过模型推理能力进行传递，对系统威胁的分析具有积极促进作用，同时提高了安全需求获取的完整性和有效性。该方法较适合在面向主体和意图的需求建模基础上获取安全需求，但此方法的实施是比较复杂的，时间耗费较多。目前，面向主体的建模工具已比较成熟，因此该方法可用性比较好。建立的威胁模型和安全需求模型有利于体现系统安全问题的特征，建立的模型可作为复用资源来帮助领域内的其他软件项目解决安全问题。

3.3.5 横切威胁的思想

作为软件需求的一个关注点，安全性经常是缠结和分散在软件的需求中。基于面向方面的思想获取安全需求，是将软件系统中可能存在威胁的地方当作“连接点”，将同一个威胁下的所有链接点组织成“横切点”，能够解决威胁的安全需求作为“通知”，将“通知”和“横切点”组织成“aspect”。目前面向方面的安全需求获取思想主要有两个典型性方法：1)Haley 等人提出的从横切威胁描述中获取安全需求的方法[3]；2)Dianxiang Xu 等人提出的基于面向方面安全需求获取方法[11,12]。

Haley 等人的方法是以问题框架分析方法为依托，系统的安全威胁存在并分散于系统的问题领域和机器领域中。问题领域中的风险资产是威胁的主要来源，问题领域间的交互是威胁的间接来源。该方法获取安全需求的主要步骤为：

1)在问题上下文中识别风险的资产。

2)依据资产所具有的安全关注点，识别资产上的威胁，获取威胁描述。

3)通过对问题领域的现象分析，判定问题领域的现象描述是否满足了威胁发生的条件，如果满足，则产生新的安全需求或者对原有需求做出修改，以阻止威胁的发生。

4)识别冲突。针对步骤 3)中安全需求的引入，判断是否有新的威胁被引入到系统中以及需求之间是否发生冲突。

方法中还采用信任假定的分析方法，假定一些问题领域是可以信任的，无安全问题发生，这可以减少威胁分析的复杂性。该方法可利用已有的问题框架方法支持工具作为该方法的支撑工具。

Dianxiang Xu 等人的方法，主要是以用例文本为分析对象，方法的主要过程是：

1)根据用例的执行流程描述识别威胁，所识别出的威胁可看作连接点。

2)组织和建立威胁用例，主要包括威胁发生事件的描述威胁连接点的描述等。

3)组织和建立安全需求用例，主要包括安全需求的描述、威胁横切点的描述等。

4)采用 Aspect 结构封装横切的威胁和安全需求。

该方法适用于在用例需求描述的文本上分析安全需求，方法还为威胁用例与安全需求用例提供了模板描述形式。采用 aspect 形式描述的横切威胁点和“通知”能够表明威胁对软件系统的横切关系以及安全需求对横切威胁的消解关系。这两种 aspects 描述与系统的功能性用例的描述相互分离，它们可作为复用的资源被领域内其他软件系统所使用。

上述两个方法都提供了威胁分析方法，但还需要安全分析人员对威胁进行确定，这直接影响了安全需求定义的完整

性和有效性。面向方面的需求分析思想适合与已有的需求分析方法相结合，只要能够确定软件系统的关注点，再提供从功能关注点中分析安全威胁的方法，就可以获取威胁并定义横切关注点。

3.3.6 CLASP 解决方案

CLASP 是 IBM 针对软件安全问题所提出的一套方法体系，其中包括安全需求的获取方法、软件安全性架构方法等一系列保障软件安全性的方法，方法适合应用在轻量级软件系统的开发过程中。这里介绍 CLASP 获取安全需求的方法。

方法一共包含 4 个步骤：

1)识别系统包含的所有资源及其拥有者。

2)依据安全关注点分类目录对资源进行分类，目录中包括隐私、信任等常见的安全关注点。

3)识别威胁。根据需求的描述，从系统资源之间的交互过程中分析资源是否存在违反安全关注点的事实。

4)针对违反安全关注点的事实，制定安全需求。

CLASP 中安全需求获取方法有相应的工具支持，目前该方法应用到许多商业领域的软件安全性保障中。该方法实质是根据资源之间的交互过程分析系统的安全问题，过程比较复杂，需要经验丰富的安全分析人员的参与。方法中提供的安全关注点分类目录是可复用的资源，方法的研究者们正积极地构建可复用的安全需求样例，以便使用者们减轻获取安全需求的任务。

3.3.7 通用标准

CC(Common Criteria)是 IT 产品安全性评测的一个通用标准，CC 一共包含 3 个部分，其中第 2 部分详细说明了系统的安全功能需求，给出了常用的安全功能类，如 FAU 类(安全审计)，FCO 类(通信)等。CC 以模板的形式描述了安全需求，使用者只需要对模板进行适当的剪裁和填充便可得到实例化的安全需求。目前已有多种方法采取与 CC 相结合的方式获取安全需求，下面介绍两个典型性方法。

Ware M 的方法[14]以需求用例文本为研究对象，为系统的参与者定义了 7 个安全相关的属性并根据属性定义了一些威胁匹配规则，分析人员只需要对属性赋值，就可以从 ECMA 的威胁类库中自动得到安全威胁，根据安全威胁库的入口可以得到每一个威胁所对应的安全目标，最后可以从 CC 安全功能类库中获取安全需求。他们对 violet 工具进行扩展，用以支持方法的实施，使用者不但可以借助 ECMA 和 CC 安全功能类库获取威胁，也可以自行通过分析得到安全威胁和安全需求，然后添加到分析结果中。该方法的好处是：使用者可轻易地获取比较有效的安全威胁和安全需求，该方法比较适合安全知识匮乏的团队使用。

Motoshi 和 Haruhiko 提出了利用 CC 知识库获取安全需求的方法[15]。将 CC 的安全功能类及其关联的 E-COFC 威胁类库作为启发式知识库。方法的主要过程是：抽取已有需求描述的属性信息；根据属性制定搜索策略；应用搜索策略，从威胁库中获取威胁以及相应的安全目标；最后依据安全目标从安全功能类库中得到安全需求。人们只需要熟悉知识库并根据搜索策略就可以得到标准的安全需求。方法的缺点是需要人工对知识库进行搜索，还缺相应的工具支持。

从以上两个方法中可以看出：基于 CC 的安全需求获取方法通过已有的知识库确定软件系统的安全威胁和安全需求，知识库在这个过程中起到关键作用，然而目前 CC 方法中的知识库受领域的限制，比如以上提到的 ECMA 和 E-COFC 是关于分布式软件系统的威胁知识库，因此方法的应用性受到了制约。

3.3.8 综合比较

对以上工作进行总结，综合比较所介绍的方法，如表 2 所列。

表 2 安全需求获取方法总体比较

方法	可用性	适用性	复用	需求描述	完整性与有效性
1. 滥用用例	工具支持、较易使用	在用例分析之上	适合	滥用用例模板的形式	安全人员决定
2. 滥用问题框架	工具支持、较易使用	在问题框架分析之上	适合	问题框架的描述形式	安全人员决定
3. 反模型	使用的代价高	在面向目标需求分析之上	不适合	扩展的 KAOS 语言	安全人员决定
4. 安全的 I*/Tropos	工具支持、较易使用	在面向主体和意图分析之上	适合	主体模型中的手段、目标、任务	安全人员决定
5. 横切威胁	工具支持、较易使用	在已有的需求分析方法之上	适合	“方面”结构的描述	安全人员决定
6. CLASP	工具支持、较易使用	商业开发，轻量级系统	适合	自然语言	安全人员决定
7. 通用标准	工具支持、较易使用	安全知识匮乏的团队	适合	模板	安全知识库起决定作用

4 存在的问题及发展趋势

获取软件系统的安全需求是开发高安全性、高可信性软件的有效途径，本文选取了典型性的安全需求获取方法，从研究途径、获取安全需求的思想两个方面对所选取的方法进行分类，并对这些方法从实用性、适用性等角度进行了分析和比较。

基于传统的需求分析思想研究安全需求的获取方法是一条有效的研究途径，这类方法弥补了传统需求分析方法的不足，能够让需求分析人员进一步地捕获软件系统的安全需求。这类方法中，除了基于面向方面的安全需求获取方法外，其余方法的共同缺点是与其所扩展的需求分析框架有较强的依赖性，比如 misuse case 方法更适合在 use case 分析之后进行安全需求的获取。尽管目前的基于面向方面的安全需求分析方法只适合应用在问题框架和用例的需求分析框架中，但对不同的需求分析方法，研究基于面向方面的安全需求获取方法是一个很大的发展空间。

研究特定的安全需求获取方法是一种创新的研究途径，本文介绍的 CLASP 方法和基于 CC 的方法都是这种研究途径的成果，它们能够有效地获取安全需求，但同时又具有局限性，CLASP 更适合应用在轻量级的商业领域中，而 CC 方法的使用受领域的限制。

除了基于 CC 的安全需求获取方法外，其余的方法都需要依靠安全分析人员来确定安全威胁和安全需求，这需要安全分析人员依靠自身的经验进行探索，探索过程类似头脑风暴式的分析过程。采用这类方法获取安全需求需要耗费较多

的时间，安全分析人员的经验和能力是安全需求有效性和完整性的关键保障。尽管如此，这类方法仍对安全需求的获取问题提供了有效的解决方案。

基于CC的安全需求获取方法只需要通过威胁知识库就可以得到领域内软件系统可能面临的安全威胁，再通过威胁库和相应的安全功能类库就可以得到标准的安全需求，该方法避免了安全分析人员头脑风暴式的分析过程，减轻了安全分析人员的负担，有利于安全分析人员匮乏的团队采用该方法获取安全需求，方法的本质是安全知识的复用。然而，这种基于复用的安全需求获取方法领域约束性较严重，因为不同领域安全知识的差异性较大。

对目前已有的安全需求获取方法进行总结，以下的3个研究方向将是今后研究的趋势和重点：

1)针对已有的需求分析方法，在其基础上研究基于面向方面的安全需求获取方法。

2)针对安全需求，研究挖掘领域内安全知识的方法和技术，建立威胁类库和相应的安全需求库，并在此基础上研究基于安全知识的安全需求获取方法。

3)针对头脑风暴式的安全需求获取方法，研究如何与知识库相结合的方法，帮助分析人员确定威胁和安全需求。

结束语 软件主动式防御可有效地构建高安全性、高可信性的软件产品，安全需求的获取在主动式防御中起着关键性作用。本文主要介绍了当前典型的安全需求获取方法，通过对方法的分析和评价，使读者能够认识方法的本质，让安全分析人员能够选取合适的方法获取安全需求，这对高安全性、高可信性的软件开发有实际指导作用。

参 考 文 献

[1] 朱鸿. 提高软件质量保障软件安全性 ——探讨21世纪计算机科学与软件产业发展战略[OL]. http://www2.ccw.com.cn/1995/37/135973.shtml,2010

[2] Yoshioka N, Hironori W, Maruyama K. A Survey on Security Pat-terns[J]. Progress in Informatics,2008(5):35-47

[3] Haley C B, Laney R C, Nuseibeh B. Deriving Security Requirements from Crosscutting Threat Descriptions[C]// Proceedings of the 3rd International Conference. New York: ACM Press, 2004:112-121

[4] Sindre G, Opdahl A L. Eliciting Secutiry Requirements with Misuse Cases [J]. Requirements Engineering,2005,10(1):34-44

[5] Alexander I F. Initial Industrial Experience of Misuse Ca-ses in Trade-Off Analysis[C]// Proceedings of the 10th Anniversary IEEE Joint International Conference. Washing-ton, DC: IEEE Computer Society,2002:61-70

[6] John M. Using Abuse Case Models for Security Requirements Analysis[C]// Proceedings of the 15th Annual Computer Security Applications Conference. Washington, DC: IEEE Computer Society,1999:55-66

[7] Lin Lun-cheng, Nusebeh B, Ince P, et al. Using Abuse Frames to Bound the Scope of Security Problems[C]// Proceedings of the Requirements Engineering Conference, 12th IEEE International. Washington,DC:IEEE Computer Society,2004:354-355

[8] Lin Luncheng,Nusebeh B,Ince P,et al. Introducing Abuse Frames for Analysing Security Requirements[C]// Proceedings of the 11th IEEE International Conference. Washington,DC:IEEE Computer Society,2003:371

[9] Lamsweerde A V. Elaborating Security Requirements by Construction of Intentional Antimodels[C]// Proceedings of the 26th International Conference on Software Engineering. Washington,DC:IEEE Computer Society,2004:148-157

[10] Liu Lin,Eric Y,John M. Security and Privacy Requirements Analysis within a Social Setting[C]// Proceedings of the International Conference on Requirements Engineering. Washington, DC:IEEE Computer Society,2003:151

[11] Xu Dian-xiang,Goel V,Nygard K E,et al. An Aspect-oriented Approach to Security Requirements Analysis[C]// Proceedings of the 30th Annual International Computer Software and Applications Conference(COMPSAC). Washington,DC: IEEE Computer Society,2006:79-82

[12] Xu Dianxiang,Goel V,Nygard K E,et al. Aspect-oriented specification of threatdriven security requirements[J]. International Journal of Computer Applications in Technology,2008,31,(1/2):131-140

[13] John V. Building Security Requirements with CLASP[J]. ACM SIGSOFT Software Engineering Notes,2005,30(4):1-7

[14] Ware M,Bowles J,Eastman C. Using the common criteria to Elicit security Requirements with use cases[C]// Proceedings of the IEEE. 2006

[15] Motoshi S, Haruhiko K. Security Requirements Elicitation Using Method Weaving and Common Criteria[M]. Heidelberg:Springer,2009:185-196

[16] Firesmith D. Security Use Cases [J]. Journal of Object Technology,2003,2(3):53-64

[17] Crook R,Ince D C,Lin Lun-cheng,et al. Security Requi-rements Engineering:When Anti-Requirements Hit the Fan[C]// Proceedings of the 10th Anniversary IEEE Joint International Conference. Washington, DC: IEEE Computer Society, 2002: 203-205

[18] Lutz R R. Software Engineering for Safety:A Roadmap[C]// Proceedings of the Conference on The Future of Software Engineering. International Conference on Software Engineering. New York:ACM Press,2000:213-226

[19] Haley C, Moffett J, Nuseibeh B. Security Requirements Engineering:A Framework for Representation and Analysis[J]. IEEE Transation on Software Engineering,2005,34(1):133-153

[20] Ashish A,Daya G. Security Requirements Elicitation Usingview Points for Online System[C]//Proceedings of the 2008 First International Conference on Emerging Trends in En-gineering and Technology. 2008

[21] McGraw G,周长发,马颖华. 软件安全-使安全成为软件开发必需的部分[M]. 北京:电子工业出版社,2008

[22] 金芝,刘璘,金英. 软件需求工程:原理和方法[M]. 北京:科学出版社,2008